Настраивал подключение centos серверов к openvpn серверу и столкнулся с неожиданной ошибкой, с которой провозился около часа, пока не нашел решение. Суть в том, что не получалось добавить tun интерфейс в зону trusted в настройках firewalld. Все простые и очевидные решения не подходили. Статья будет в тему вопроса, почему я не использую firewalld, а продолжаю писать правила в классическом iptables.

У меня есть openvpn сервер и пачка других серверов с centos, которые надо объединить приватной сетью между собой. Настроил сервер по своей же статье - настройка openvpn. Подключил клиентов к серверу, они нормально видят друг друга, сеть работает. Дальше нужно было отключить некоторые сервисы из публичной сети и разрешить их работу только через openvpn. Задача простейшая - закрываем доступ к определенным портам из интернета, разрешаем все в сети openvpn, которая использует tun интерфейс.

Для справки приведу все команды, которыми пользовался, может кому-то пригодится. Покажу на примере сервиса мониторинга zabbix, который использует tcp порт 10050. Для начала сморим список всего, что разрешено на фаерволе:

```
# firewall-cmd --permanent --list-all

public
 target: default
 icmp-block-inversion: no
 interfaces:
 sources:
 services: ssh dhcpv6-client http https
 ports: 22987/tcp 8070/tcp 80/tcp 443/tcp 8890/tcp 8891/tcp 8893/tcp 8894/tcp 5222/tcp 5223/tcp 10050/tcp
 protocols:
 masquerade: no
 forward-ports:
```

```
  source-ports:
  icmp-blocks:
  rich rules:
```

У меня получился такой список. Мне нужно отключить службу ssh и 10050/tcp порт. Они не нужны в публичной сети. Заодно уберем dhcpv6-client, он тоже не нужен. Отключаем:

```
# firewall-cmd --permanent --zone=public --remove-service=dhcpv6-client
# firewall-cmd --permanent --zone=public --remove-service=ssh
# firewall-cmd --permanent --zone=public --remove-port=10050/tcp
```

Сохраняем правила:

```
# firewall-cmd --reload
```

Теперь мне нужно добавить всю vpn сеть в список доверенных сетей, чтобы не открывать отдельно каждый порт. Для начала смотрим список активных сетей в данный момент:

```
# firewall-cmd --get-active-zones

bx_trusted
  sources: 193.121.174.217/32
public
  interfaces: eth0
```

bx_trusted создает bitrixenv после установки на сервер. В данном случае не принципиально. Нам нужно добавить еще одну активную зону trusted с интерфейсом tun0. Нет ничего проще:

```
# firewall-cmd --permanent --zone=trusted --add-interface=tun0

The interface is under control of NetworkManager and already bound to 'trusted'
The interface is under control of NetworkManager, setting zone to 'trusted'.
success
```

Двоякое чувство. Сначала написали подозрительное сообщение, потом сказали, что success. Проверяю еще раз список активных зон - ничего не изменилось. Дальше пошел в гугль. Тема популярна, решение тоже предлагается, в том числе где-то на сайте redhat. Либо отключите управление NetworkManager сетевым интерфейсом, либо явно пропишите зону для интерфейса. Делается все это в конфигурационном файле в директории */etc/sysconfig/network-scripts*. Делается это либо так:

```
NM_CONTROLLED=no
```

либо вот так:

```
ZONE=trusted
```

Все бы хорошо, но интерфейс tun0 поднимается после запуска openvpn клиента и конфигурационного файла у него нет. Более того, если в консоли запустить nmtui - утилиту NetworkManager для управления сетью, там вы тоже не найдете tun. Ситуация странная и неоднозначная. Мне изначально хотелось все сделать, сохранив дефолтную установку системы - не отключать NetworkManager и Firewalld. Время от времени я получаю информацию о том, что это удобно и надо привыкать к новым средствам, которые сделаны, чтобы облегчить жизнь системных администраторов.

Я честно пытался себе облегчить жизнь, но в итоге не выдержал и отключил NetworkManager:

```
# systemctl stop NetworkManager
# systemctl disable NetworkManager
```

```
# systemctl restart network
```

После этого снова добавил tun0 в зону trusted:

```
# firewall-cmd --permanent --zone=trusted --add-interface=tun0
success
```

Никаких подозрительных сообщений не получил. Сохранил правила firewalld:

```
# firewall-cmd --reload
```

И проверил, применились ли изменения:

```
# firewall-cmd --get-zone-of-interface=tun0
trusted

# firewall-cmd --get-active-zones
bx_trusted
 sources: 193.121.174.217/32
public
 interfaces: eth0
trusted
 interfaces: tun0
```

Все в порядке. На всякий случай проверим сами правила iptables:

```
# iptables -L -v -n | grep tun
 0 0 FWDI_trusted all -- tun0 * 0.0.0.0/0 0.0.0.0/0
 0 0 FWDO_trusted all -- * tun0 0.0.0.0/0 0.0.0.0/0
 0 0 IN_trusted all -- tun0 * 0.0.0.0/0 0.0.0.0/0
```

Теперь точно все в порядке. Для проверки перезагрузил сервер. Все настройки сохранились, туннель поднялся, сервисы заработали через openvpn.

Это не первая ситуация, когда я трачу время на то, чтобы решить проблему с firewalld. Я искренне не понимаю, чем он удобнее классических правил iptables. Мне достаточно один раз посмотреть скрипт конфигурации iptables, чтобы увидеть всю картину, быстро что-то добавить или изменить и применить изменения. И такой ерунды, как в приведенном мной примере никогда не было. Все работает четко и понятно.

А как вы считаете NetworkManager и Firewalld лучше и удобнее традиционных средств управления сетью и фаерволом? Я в упор не вижу простоты и удобства. Точно так же не вижу удобства ip в сравнении с ifconfig и netstat. К ip я уже привык, как к замене ifconfig, сетью управляю только через ip. Но вот вывод аналогичной информации netstat через ip получается менее наглядным и удобным. По прежнему использую netstat.

Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоем распоряжении. Расскажи, как сделать правильно!

Помогла статья? Подписывайся на telegram канал автора

Анонсы всех статей, плюс много другой полезной и интересной информации, которая не попадает на сайт.